



U.S. Department of Justice

*United States Attorney
Southern District of New York*

*The Silvio J. Mollo Building
One Saint Andrew's Plaza
New York, New York 10007*

December 13, 2019

BY ECF

The Honorable Paul A. Crotty
United States District Judge
Southern District of New York
500 Pearl Street
New York, New York 10007

Re: *United States v. Dawdu Marriott*, S1 18 Cr. 339 (PAC)

Dear Judge Crotty:

The defendant in the above-captioned case is scheduled to be sentenced on December 19, 2019, at 10:30 a.m. The Government respectfully submits this letter in connection with sentencing. For the reasons set forth below, the Court should impose a sentence within the Stipulated Guidelines Range of 57 to 65 months' imprisonment.

I. Offense Conduct

Marriott and his co-conspirators participated in a wide-ranging scheme (the "Fraud Scheme") that involved unlawfully obtaining personally identifiable information of other individuals (including names, addresses, phone numbers, email addresses, birthdates, Social Security numbers, bank account numbers, credit and debit card numbers, and cellphone service provider account numbers); impersonating those individuals in order to obtain unauthorized access to their bank, credit and debit card, and cellphone service provider accounts; using such access to, among other things, facilitate the fraudulent transfer of funds to other bank accounts controlled by members of the conspiracy and the unauthorized purchasing of merchandise and gift cards at retail stores. In total, members of the conspiracy unlawfully obtained more than \$3,500,000 and attempted to obtain a total of more than \$6,000,000.

To carry out the Fraud Scheme, members of the conspiracy obtained victims' personally identifiable information from various sources, including the dark web and commercial establishments at which members of the scheme worked. For example, one of Marriott's co-defendants, Jillian Walcott, stole victims' personally identifiable information from an urgent care walk-in medical clinic in Manhattan where she worked. After obtaining a victim's personally identifiable information, conspirators typically manufactured fraudulent credit or debit cards linked to victims' accounts at financial institutions in order to access those accounts to make fraudulent purchases or wire transfers.

In some cases, members of the conspiracy attempted to “port”¹ (i.e., transfer) a victim’s telephone number to a cellphone controlled by a Fraud Scheme participant. Once the victims’ telephone numbers were “ported” to cellphones controlled by Fraud Scheme participants, the Fraud Scheme participants would place telephone calls from those cellphones (to which the recently ported numbers were assigned) to the victims’ financial institutions. In most cases, the relevant financial institution’s telephone system automatically recognized the incoming telephone numbers as belonging to their account holders and, on that basis, required fewer pieces of identifying information to authenticate the identity of the callers. The defendants and/or their co-conspirators answered the limited set of authentication questions posed by the financial institution’s customer service representative and then requested that (a) funds be sent via wire transfer to various accounts with other financial institutions and/or (b) “replacement” credit cards be sent to an address not associated with the account holder. In other cases, Fraud Scheme participants used the “ported” cellphones to approve fraudulent purchases when a victim’s financial institution texted or called a victim’s telephone number to verify the propriety of the fraudulent purchases.

Marriott’s role in the scheme was to purchase and assist with purchasing stolen personally identifiable information, including bank account information, from the internet and supply it to co-conspirators who would use that information to, among other things, access victims’ bank and credit card accounts and manufacture counterfeit credit cards to fraudulently purchase merchandise. Wiretap interceptions of Marriott include a conversation on June 28, 2017, with co-defendant Melvin Brown:

- BROWN: Yo
- MARRIOTT: I only found them 2 BINS² on the site. Them other BINS [unintelligible].
- BROWN: You haven't sent me a number yet nigga.
- MARRIOTT: You wanted me to buy them?
- BROWN: Hell yea, [unintelligible] a couple dollars my nigga.
- MARRIOTT: You should've told me that. You didn't say nothing from this morning.

¹ “Porting” refers to a formal technical process whereby an existing telephone number is reassigned to a different cellphone. Initiating the porting process without authorization of the owner of the cellphone number is a critical aspect of the scheme described herein, because credit card issuers often contact their customers via the cellphone number on file when the issuer detects suspicious activity on a customer’s account. If a member of the scheme has control of the cellphone number, then that member can falsely confirm the propriety of fraudulent transactions.

² In this context, “BINS” refers to Bank Identification Numbers.

- BROWN: [unintelligible] last night was too late or some shit like that.
- MARRIOTT: The money ready on the site. The money ready on the site.
- BROWN: I know. I know. How much you got, how much still on there?
- MARRIOTT: How much still on there? I gotta pull it up on my labby.³

During another call with Brown later that same day, Marriott informed Brown that Marriott “just sent 5 and I am going to send like 5 more,” which refers to individually identifiable information of other individuals purchased on the internet. There are several other intercepted conversations during which Marriott and Brown appeared to discuss purchasing stolen individually identifiable information on the internet, and text messages and photographs they had apparently exchanged concerning information relating to the scheme, such as individually identifiable information of potential victims and the status of credit cards that Brown and Marriott appeared to have compromised.

On May 23, 2018, law enforcement agents executed a search warrant at Marriott’s residence in Margate, Florida. Law enforcement agents recovered, among other things, a credit card embosser, a box of blank checks, six laptops, and eight cellphones (including the cellphone used by Marriott in the above-mentioned wiretapped calls).

II. Procedural History

On February 27, 2019, Marriott was charged in Superseding Indictment S1 18 Cr. 339 (PAC) (the “Indictment”) with conspiracy to commit access device fraud, in violation of Title 18, United States Code, Section 1029(b)(2) (Count One); conspiracy to commit wire fraud, in violation of Title 18, United States Code, Section 1349 (Count Two); and aggravated identity theft, in violation of Title 18, United States Code, Section 1028A (Count Three). (PSR ¶¶ 1-4.)⁴ On August 19, 2019, Marriott pled guilty to Count Two and Count Three of the Indictment pursuant to a plea agreement. (PSR ¶ 6.) In the plea agreement, the parties stipulated that the offense level for Count Two is 18, that the defendant’s Criminal History Category is III, and that the Guidelines Range for Count Two is 33 to 41 months’ imprisonment, plus an additional 24 months’ consecutive sentence for Count Three. (PSR ¶ 7.) The Probation Office reached the same conclusion with respect to the Guidelines calculation. (PSR ¶ 118)

³ In this context, “labby” refers to laptop computer.

⁴ “PSR” refers to the draft presentence report issued on November 22, 2019. The final presentence report has not yet been issued by the Probation Office.

III. Sentences Imposed on Co-Defendants

To assist the Court in assessing the relative culpability of the defendants, the Government provides the following chart of the defendants who have pled guilty in this case, listed approximately in their order of culpability (from most to least culpable):

Defendant	Criminal History Category	Criminal Offenses	Mandatory Minimum (months)	Guidelines Range (months)	Sentence of Imprisonment (months)
Jamal Simon	I	wire fraud conspiracy; aggravated identity theft; wrongfully obtaining individually identifiable health information	24	121 to 155	
Melvin Brown	IV	wire fraud conspiracy; aggravated identity theft	24	65 to 75	
Dawdu Marriott	III	wire fraud conspiracy; aggravated identity theft	24	57 to 65	
David Boyd	IV	wire fraud conspiracy; aggravated identity theft	24	51 to 57	51
Rashaun McKay	III	wire fraud conspiracy; aggravated identity theft	24	51 to 57	
Dwayne Norville	IV	wire fraud conspiracy	0	33 to 41	28
Jillian Walcott	I	wire fraud conspiracy; wrongfully obtaining individually identifiable health information	0	33 to 41	

Defendant	Criminal History Category	Criminal Offenses	Mandatory Minimum (months)	Guidelines Range (months)	Sentence of Imprisonment (months)
Megan Montoya	III	wire fraud conspiracy	0	33 to 41	Time Served (83 days)
Darren Davidson	I	wire fraud conspiracy	0	27 to 33	
Yvette Lubrun	I	wire fraud conspiracy	0	15 to 21	Probation

IV. Discussion

A. Applicable Law

Although *United States v. Booker* held that the Guidelines are no longer mandatory, it also held that they remain in place and that district courts must “consult” the Guidelines and “take them into account” when sentencing. 543 U.S. 220, 264 (2005). As the Supreme Court stated, “a district court should begin all sentencing proceedings by correctly calculating the applicable Guidelines range,” which “should be the starting point and the initial benchmark.” *Gall v. United States*, 552 U.S. 38, 49 (2007).

After that calculation, a sentencing judge must consider seven factors outlined in Title 18, United States Code, Section 3553(a): (1) “the nature and circumstances of the offense and the history and characteristics of the defendant;” (2) the four legitimate purposes of sentencing, as set forth below; (3) “the kinds of sentences available;” (4) the Guidelines range itself; (5) any relevant policy statement by the Sentencing Commission; (6) “the need to avoid unwarranted sentence disparities among defendants;” and (7) “the need to provide restitution to any victims.” 18 U.S.C. § 3553(a)(1)-(7); *see also Gall*, 552 U.S. at 50 & n.6.

In determining the appropriate sentence, the statute directs judges to “impose a sentence sufficient, but not greater than necessary, to comply with the purposes” of sentencing, which are:

- (A) to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offense;
- (B) to afford adequate deterrence to criminal conduct;
- (C) to protect the public from further crimes of the defendant; and
- (D) to provide the defendant with needed educational or vocational training, medical care, or other correctional treatment in the most effective manner.

18 U.S.C. § 3553(a)(2).

B. A Guidelines Sentence Is Appropriate In This Case

The 18 U.S.C. § 3553(a) factors particularly applicable here include the need for the sentence to reflect the nature and seriousness of the offense, to afford adequate deterrence to this defendant and others who are similarly situated, to promote respect for the law, and to protect the

public from further crimes of the defendant. 18 U.S.C. § 3553(a)(2)(A)-(C). These considerations weigh in favor of a sentence within the Guidelines Range of 57 to 65 months' imprisonment.

First, a sentence within the Guidelines Range would appropriately reflect the nature and seriousness of the defendant's conduct. The defendant played a critical role in the Fraud Scheme, as one of the sources of stolen individually identifiable information that enabled the members of the Fraud Scheme to steal the identities of innocent victims and use those identities to their own financial benefit, at the cost of financial institutions and the victims. Marriot's role was significant, as was evidenced by the items recovered by law enforcement agents from his home: a credit card embosser, a box of blank checks, six laptops (at least one of which contained images of thousands of prospective victims' checks), and eight cellphones (including the cellphone used by Marriott in the above-mentioned wiretapped calls). In total, Marriott is responsible for between \$150,000 and \$250,000 in losses to victims. (PSR ¶ 49.) Overall, the Fraud Scheme caused losses of more than \$3.5 million to victims and attempted to scam millions more.

Second, a sentence within the Guidelines Range is necessary to promote respect for the law and to deter others who are similarly situated from participating in similar schemes. Fraud schemes of this type are on the rise because the unscrupulous have found that identity theft is profitable and easy to implement and conceal from law enforcement. Following the nominal investment in obtaining individually identifiable information and blank cards with magnetic strips, the crime carries no further financial cost, apart from the prospect of apprehension and criminal penalties. However, the likelihood of detection is substantially lower than many other theft offenses. Victims often do not realize that have been victimized for some period and are not able to report the fraud until well after funds have been stolen from their accounts and they have been substantially harmed. In addition, the investigation of cases such as these is extraordinarily resource-intensive for law enforcement, and requires a substantial investment of resources in order to reveal the activities of a scheme such as this and the identities of its members. Substantial punishment is required to counterbalance the general perception that this type of scheme carries low costs for perpetrators.

Third, a sentence within the Guidelines Range is needed to deter this defendant from committing additional crimes and to protect the public. The defendant's criminal history, which includes more than a dozen convictions, is lengthy and serious. His most alarming conduct includes a conviction for attempted robbery, for which he was sentenced to 18 months' probation (PSR ¶ 72). In addition, while on probation from the attempted robbery conviction, the defendant was observed shoplifting. (PSR ¶ 74.) When a security guard responded, the defendant menaced the guard with a razor knife, used physical force to retain the property he was attempting to steal, and caused injury to the security guard. (PSR ¶ 74.) The defendant was sentenced to 90 days' imprisonment. (PSR ¶ 74.)

The defendant's prior criminal conduct is troubling. He has violated the conditions of several terms of parole and probation, and he has several theft and drug related convictions. He has served several stints in prison, ranging from just a few days to up to a year at a time. Alarming, none of those experiences with the criminal justice system appear to have had any deterrent effect on the defendant at all. Indeed, the current criminal conduct was committed just a couple of years after his most recent term of probation expired. (See PSR ¶ 85.) The Court should

sentence the defendant to a term of imprisonment within the Guidelines Range to ensure that the defendant is adequately deterred and to protect the public from his pattern of crime for a meaningful period.

In sum, a sentence within the Guidelines Range adequately would balance the various considerations under § 3553(a) and achieve the statute's stated objectives.


V. Conclusion

For the reasons set forth above, the Government respectfully requests that the Court impose a sentence on the defendant within the Guidelines Range of 57 to 65 months' imprisonment, as such a sentence would be sufficient but not greater than necessary to serve the legitimate purposes of sentencing.

Respectfully submitted,

GEOFFREY S. BERMAN
United States Attorney

By:



Nicholas W. Chiuchio
Robert B. Sobelman
Assistant United States Attorneys
(212) 637-1247/2616

Cc: Kenneth J. Montgomery, Esq. (by ECF)